In the Claims:

Claims 1-25 (Canceled).

26. (Previously Presented) A system for providing continuous authentication of a user of a computing device, comprising:

a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

securely-stored biometric information which identifies an owner of the computing device;

means for repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device, wherein the means for repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation;

means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

means for concluding, within a security core, that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core remaining securely operably connected until completion of the security-sensitive operation.

27. (Previously Presented) A system for providing continuous authentication of a user of a computing device, comprising:

a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

securely-stored biometric information which identifies an owner of the computing device;

means for repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device, wherein the means for repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation;

means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

means for concluding, within a security core, that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remaining securely operably connected until completion of the security-sensitive operation.

Claims 28-59 (Canceled).

60. (Previously Presented) A method for providing continuous authentication of a user of a computing device, comprising:

operating a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device, wherein the repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

concluding with a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core remaining securely operably connected until completion of the security-sensitive operation.

61. (Previously Presented) A method for providing continuous authentication of a user of a computing device, comprising:

operating a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device, wherein the repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

concluding within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remaining securely operably connected until completion thereof.

Claims 62-93 (Canceled).

94. (Previously Presented) A computer program product for providing continuous authentication of a user of a computing device, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code that is configured to operate a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

computer-readable program code that is configured to access a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

computer-readable program code that is configured to access securely-stored biometric information which identifies an owner of the computing device;

computer-readable program code that is configured to repeatedly obtain, from the biometric sensor component, biometric input of a user of the computing device, and to be activated upon beginning a security-sensitive operation and terminated upon completion of the security-sensitive operation;

computer-readable program code that is configured to compare the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

computer-readable program code that is configured to conclude within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core remaining securely operably connected until completion of the security-sensitive operation.

95. (Previously Presented) A computer program product for providing continuous authentication of a user of a computing device, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code that is configured to operate a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

computer-readable program code that is configured to access a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

computer-readable program code that is configured to access securely-stored biometric information which identifies an owner of the computing device;

computer-readable program code that is configured to repeatedly obtain, from the biometric sensor component, biometric input of a user of the computing device, and to be activated upon beginning a security-sensitive operation and terminated upon completion of the security-sensitive operation;

computer-readable program code that is configured to compare the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

computer-readable program code that is configured to conclude within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remaining securely operably connected until completion thereof.

Claims 96-102 (Canceled).

103. (Previously Presented) A method of doing business by continually authenticating a user of a computing device, comprising:

operating a security component for the computing device, wherein the security component provides security functions such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

performing a security-sensitive operation using the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device over a duration of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user;

determining within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and

which are involved in the security-sensitive operation remaining securely operably connected until completion of the security-sensitive operation; and

aborting the security-sensitive operation if the comparing ~~step~~ fails at any time over the duration of the security-sensitive operation or if the security-sensitive operation is determined not to be authentic.

104. (Previously Presented) A method of improving security of a computing device, comprising:

operating a security component for the computing device, wherein the security component provides security functions such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner;

performing a security-sensitive operation using the computing device; and

determining within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remaining securely operably connected until completion of the security-sensitive operation.

105. (Previously Presented) A method of improving security of operations carried out with a computing device, comprising:

operating a security component for the computing device, wherein the security component provides security functions such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

performing a security-sensitive operation using the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device over a duration of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

determining within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remaining securely operably connected until completion of the security-sensitive operation.